

- Rossow, Kurt Thomas, Vern Paxson, Stefan Savage, and Geoffrey M. Voelker. Manufacturing Compromise: The Emergence of Exploit-as-a-service. In *Proc. of the ACM Conference on Computer and Communications Security (CCS)* (2012).
- [31] Felix Gröbert, Carsten Willems, and Thorsten Holz. Automated Identification of Cryptographic Primitives in Binary Programs. In *Proc. of the International Symposium on Recent Advances in Intrusion Detection (RAID)* (2011).
- [32] Andreas Haas, Andreas Rossberg, Derek L. Schuff, Ben L. Titzer, Michael Holman, Dan Gohman, Luke Wagner, Alon Zakai, and JF Bastien. Bringing the Web Up to Speed with WebAssembly. In *Proc. of the ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI)* (2017).
- [33] John J. Hoffman, Steve C. Lee, and Jeffrey S. Jacobson. New Jersey Division of Consumer Affairs Obtains Settlement with Developer of Bitcoin-Mining Software Found to Have Accessed New Jersey Computers Without Users' Knowledge or Consent. <https://nj.gov/oag/newsreleases15/pr20150526b.html> (May 2015).
- [34] Danny Yuxing Huang, Hitesh Dharmdasani, Sarah Meiklejohn, Vacha Dave, Chris Grier, Damon Mccoy, Stefan Savage, Nicholas Weaver, Alex C. Snoeren, and Kirill Levchenko. Bitcoin: Monetizing Stolen Cycles. In *Proc. of the Network and Distributed System Security Symposium (NDSS)* (2014).
- [35] Simon Kenin. Mass MikroTik Router Infection – First we cryptojack Brazil, then we take the World? <https://www.trustwave.com/Resources/SpiderLabs-Blog/Mass-MikroTik-Router-Infection---First-we-cryptojack-Brazil,-then-we-take-the-World-/> (August 2018).
- [36] Brian Krebs. Who and What is Coinhive? <https://krebsonsecurity.com/2018/03/who-and-what-is-coinhive/> (March 2018).
- [37] McAfee Labs. McAfee Labs Threats Report. <https://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2014.pdf> (June 2014).
- [38] Pierre Lestringant, Frédéric Guihéry, and Pierre-Alain Fouque. Aligot: Cryptographic Function Identification in Obfuscated Binary Programs. In *Proc. of the ACM Symposium on Information, Computer and Communications Security (ASIACCS)* (2015).
- [39] Shannon Liao. Showtime websites secretly mined user CPU for cryptocurrency. <https://www.theverge.com/2017/9/26/16367620/showtime-cpu-cryptocurrency-monero-coinhive/> (September 2017).
- [40] Shannon Liao. UNICEF wants you to mine cryptocurrency for charity. <https://www.theverge.com/2018/4/30/17303624/unicef-mining-cryptocurrency-charity-monero/> (April 2018).
- [41] Chaoying Liu and Joseph C. Chen. Cryptocurrency Web Miner Script Injected into AOL Advertising Platform. <https://blog.trendmicro.com/trendlabs-security-intelligence/cryptocurrency-web-miner-script-injected-into-aol-advertising-platform/> (April 2018).
- [42] Federico Maggi, Marco Balduzzi, Ryan Flores, Lion Gu, and Vincenzo Ciancaglini. Investigating Web Defacement Campaigns at Large. In *Proc. of the ACM Asia Conference on Computer and Communications Security (ASIACCS)* (2018).
- [43] Alecia M. McDonald and Lorrie Faith Cranor. Americans' Attitudes About Internet Behavioral Advertising Practices. In *Proc. of the ACM Workshop on Privacy in the Electronic Society (WPES)* (2010).
- [44] Andrey Meshkov. Crypto-Streaming Strikes Back. <https://blog.adguard.com/en/crypto-streaming-strikes-back/> (December 2017).
- [45] Troy Mursch. Cryptojacking malware Coinhive found on 30,000+ websites. <https://badpackets.net/cryptojacking-malware-coinhive-found-on-30000-websites/> (November 2017).
- [46] Troy Mursch. How to find cryptojacking malware. <https://badpackets.net/how-to-find-cryptojacking-malware/> (February 2018).
- [47] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. <https://www.bitcoin.org/bitcoin.pdf> (2009).
- [48] Nick Nikiforakis, Luca Invernizzi, Alexandros Kapravelos, Steven Van Acker, Wouter Joosen, Christopher Kruegel, Frank Piessens, and Giovanni Vigna. You Are What You Include: Large-scale Evaluation of Remote Javascript Inclusions. In *Proc. of the ACM Conference on Computer and Communications Security (CCS)* (2012).
- [49] Lindsey O'Donnell. Cryptojacking Attack Found on Los Angeles Times Website. <https://threatpost.com/cryptojacking-attack-found-on-los-angeles-times-website/130041/> (February 2018).
- [50] Lindsey O'Donnell. Cryptojacking Campaign Exploits Drupal Bug, Over 400 Websites Attacked. <https://threatpost.com/cryptojacking-campaign-exploits-drupal-bug-over-400-websites-attacked/131733/> (May 2018).
- [51] Panagiotis Papadopoulos, Panagiotis Ilia, and Evangelos P. Markatos. Truth in Web Mining: Measuring the Profitability and Cost of Cryptominers as a Web Monetization Model. arXiv:1806.01994v1 [cs.CR] (June 2018).
- [52] Panagiotis Papadopoulos, Nicolas Kourtellis, and Evangelos P. Markatos. The Cost of Digital Advertisement: Comparing User and Advertiser Views. In *Proc. of the World Wide Web Conference (WWW)* (2018).
- [53] Giancarlo Pellegrino, Christian Rossow, Fabrice J. Ryba, Thomas C. Schmidt, and Matthias Wählisch. Cashing Out the Great Cannon? On Browser-Based DDoS Attacks and Economics. In *Proc. of the USENIX Workshop on Offensive Technologies (WOOT)* (2015).
- [54] Pirate Bay. Miner. <https://thepiratebay.org/blog/242> (September 2017).
- [55] Niels Provos, Panayiotis Mavrommatis, Moheeb Abu Rajab, and Fabian Monrose. All Your iFRAMES Point to Us. In *Proc. of the USENIX Security Symposium* (2008).
- [56] Niels Provos, Dean McNamee, Panayiotis Mavrommatis, Ke Wang, and Nagendra Modadugu. The Ghost in the Browser Analysis of Web-based Malware. In *Proc. of the Workshop on Hot Topics in Understanding Botnets (HotBots)* (2007).
- [57] Jan Rühl, Torsten Zimmermann, Konrad Wolsing, and Oliver Hohlfeld. Digging into Browser-based Crypto Mining. In *Proc. of the ACM Internet Measurement Conference (IMC)* (2018). (Preprint: <https://arxiv.org/abs/1808.00811v1>).
- [58] Salon. FAQ: What happens when I choose to "Suppress Ads" on Salon? <https://www.salon.com/about/faq-what-happens-when-i-choose-to-suppress-ads-on-salon> (2018).
- [59] Jérôme Segura. Malicious cryptomining and the blacklist conundrum. <https://blog.malwarebytes.com/threat-analysis/2018/03/malicious-cryptomining-and-the-blacklist-conundrum/> (March 2018).
- [60] Jérôme Segura. The state of malicious cryptomining. <https://blog.malwarebytes.com/cybercrime/2018/02/state-malicious-cryptomining/> (March 2018).
- [61] Seigen, Max Jameson, Tuomo Nieminen, Neocortex, and Antonio M. Juarez. CryptoNight Hash Function. <https://cryptonote.org/cns/cns008.txt> (March 2013).
- [62] Denis Sinegubko. Hacked Websites Mine Cryptocurrencies. <https://blog.sucuri.net/2017/09/hacked-websites-mine-cryptocurrencies.html> (September 2017).
- [63] Slushpool. Stratum Mining Protocol. <https://slushpool.com/help/manual/stratum-protocol> (2016).
- [64] Rashid Tahir, Muhammad Huzaifa, Anupam Das, Mohammad Ahmad, Carl Gunter, Fareed Zaffar, Matthew Caesar, and Nikita Borisov. Mining on Someone Else's Dime: Mitigating Covert Mining Operations in Clouds and Enterprises. In *Proc. of the International Symposium on Recent Advances in Intrusion Detection (RAID)* (2017).
- [65] Iain Thomson. Pulitzer-winning website Politifact hacked to mine crypto-coins in browsers. https://www.theregister.co.uk/2017/10/13/politifact_mining_cryptocurrency/ (October 2017).
- [66] Mircea Trofin. Chromium Code Reviews Issue 2656103003: [wasm] flag for asm-wasm investigations. <https://codereview.chromium.org/2656103003/> (January 2017).
- [67] Alejandro Viquez. Opera introduces bitcoin mining protection in all mobile browsers – here's how we did it. <https://blogs.opera.com/mobile/2018/01/opera-introduces-bitcoin-mining-protection-mobile-browsers/> (January 2018).
- [68] Luke Wagner. Turbocharging the Web. *IEEE Spectrum* (December 2017). (Online version: <https://spectrum.ieee.org/computing/software/webassembly-will-finally-let-you-run-high-performance-applications-in-your-browser/>).
- [69] Wenhao Wang, Benjamin Ferrell, Xiaoyang Xu, Kevin W. Hamlen, and Shuang Hao. SEISMIC: SECure In-lined Script Monitors for Interrupting Cryptojacks. In *Proc. of the European Symposium on Research in Computer Security (ESORICS)* (2018).
- [70] Web Hypertext Application Technology Working Group. HTML Living Standard: Web workers. <https://html.spec.whatwg.org/multipage/workers.html> (2018).
- [71] Chris Williams. UK ICO, USCourts.gov... Thousands of websites hijacked by hidden crypto-mining code after popular plugin pwned. http://www.theregister.co.uk/2018/02/11/browsealoud_compromised-coinhive/ (February 2018).
- [72] Dongpeng Xu, Jiang Ming, and Dinghao Wu. Cryptographic Function Detection in Obfuscated Binaries via Bit-Precise Symbolic Loop Mapping. In *Proc. of the IEEE Symposium on Security and Privacy (S&P)* (2017).
- [73] Yandex. Yandex Browser Strengthens Cryptocurrency Mining Protection. <https://yandex.com/company/blog/yandex-browser-strengthens-cryptocurrency-mining-protection/> (March 2018).
- [74] Zhang Zaifeng. Who is Stealing My Power III: An Adnetwork Company Case Study. <https://blog.netlab.360.com/who-is-stealing-my-power-iii-an-adnetwork-company-case-study-en/> (February 2018).
- [75] Apostolis Zarras, Alexandros Kapravelos, Gianluca Stringhini, Thorsten Holz, Christopher Kruegel, and Giovanni Vigna. The Dark Alleys of Madison Avenue: Understanding Malicious Advertisements. In *Proc. of the ACM Internet Measurement Conference (IMC)* (2014).
- [76] Tianwei Zhang, Yinqian Zhang, and Ruby B. Lee. CloudRadar: A Real-Time Side-Channel Attack Detection System in Clouds. In *Proc. of the International Symposium on Recent Advances in Intrusion Detection (RAID)* (2016).
- [77] Zeljka Zorz. How a URL shortener allows malicious actors to hijack visitors' CPU power. <https://www.helpnetsecurity.com/2018/05/23/url-shortener-cryptojacking/> (May 2018).